Claim Amendments

Claim 1 (currently amended): A system to establish a trusted and decentralized peer-to peer network comprising:

communication means;

n user computing devices connected to the communication means, where n is greater than or equal to 3 and is an integer; and

a host computing device connected to the communication means having a mechanism to establish a decentralized trusted communications network with at least 2 of the n user computing devices through which digital signals are shared securely between the host computing device and the 2 user computing devices of the trusted communications network, the host computer sending a public key to a first of the 3 user computing devices and the first user computing device sending the public key to a second of the 3 user computing devices and a third of the 3 user computing devices through the communication means to establish the decentralized trusted network, the host computing device identifiable to the n user computing devices, the n user computing devices and the host computing device forming a trusted member list that each user computing device has and each user computing device knows and

can communicate directly with all the other user computing devices and the host computing device on the trusted peer-to-peer network since the host computing device and all the other user computing devices have the public key, the second ~~computer~~ user computing device either accepting or denying the public key in regards to joining the decentralized trusted network, the first computing device sends a search request to the other computing devices of the trusted member list for a desired computer file via the communication means, the second user computing device having the desired computer file responds to the search request and sends the desired computer file to the first user computing device.

Claim 2 (currently amended): A method for establishing a trusted and decentralized peer-to-peer network comprising the steps of:

sending a public key from a host computing device to communication means connected to the host computing device;

receiving the public key at a first user computing device of n computing devices, where n is an integer greater than or equal to 3, connected to the communication means;

sending the public key from the first user computing device to a second user computing device connected to the communication means;

receiving the public key at the second user computing device;

sending the public key from the first user computing device to a third user computing device connected to the communication means;

receiving the public key at the third user computing device;

either denying or accepting the public key by the second user to establish a decentralized trusted communications network between the host computing device, the first, the second computing device and the third computing device through which digital signals are shared securely between the host computing device, the first user computing device, the second user computing device and the third user computing device; **[[and]]**

sending digital signals directly from the host computing device securely to the first, second and third user computing devices when the second user computing device has accepted the public key since the host computing device and the first, second and third user computing devices have the public key, the host computing device identifiable to the n user

computing devices, the n computing devices and the host computing device forming a trusted member list that each computing device has and each computing device knows the other computing devices on the trusted peer-to-peer network[[.]];

sending a search request for a desired computer file from the first user computing device to the other computing devices of the trusted member list via the communication means;

receiving the search request by the second user computing device having the desired file; and

sending the desired computer file to the first user computing device from the second user computing device via the communication means.

Claim 3 (previously presented): A method as described in Claim 2 including the step of creating encryption and decryption keys.

Claim 4 (previously presented): A method as described in Claim 3 including the step of creating a searchable ciphertext file containing identifiable network information on each computing device.

Claim 5 (previously presented): A method as described in Claim 4 wherein the creating step includes the step of creating a searchable ciphertext file containing identifiable network information on each computing device which is shared with every other computing device.

Claim 6 (previously presented): A method as described in Claim 5 including the step of finding by a member of the trusted peer-to-peer network other members of the trusted peer-to-peer network.

Claim 7 (previously presented): A method as described in Claim 6 including the step of establishing entrusted secure chat sessions between the members through the trusted peer-to-peer network.

Claim 8 (previously presented): A method as described in Claim 6 including the step of searching for a file by the member in the other members through the trusted peer-to-peer network.

Claim 9 (previously presented): An apparatus as described in Claim 1 wherein each computing device has a peer-to-peer network program, the peer-to-peer network program

of the computing device interacts through the communication means with the peer-to-peer network of every other computing device to establish the trusted peer-to-peer network.

Claim 10 (previously presented): A system as described in Claim 9 wherein the peer-to-peer network program shares the public key with the peer-to-peer network program of every other computing device.

Claim 11 (previously presented): A system as described in Claim 10 wherein each computing device has a chat protocol for establishing chat sessions with the other computing devices.

Claim 12 (previously presented): A system as described in Claim 10 wherein each computing device has a file sharing protocol which executes a search and retrieval of a computer file located in one of the other computing devices.

Claim 13 (currently amended): A method for establishing a trusted and decentralized peer-to-peer network comprising the steps of:

sending a public key from a host computing device to communication means connected to the host computing device;

receiving the public key at a first user computing device of n computing devices, where n is an integer greater than or equal to 3, connected to the communication means;

sending the public key from the first user computing device to a second user computing device connected to the communication means;

sending the public key from the first user computing device to a third user computing device connected to the communication means;

receiving the public key at the third user computing device;

receiving the public key at the second user computing device to establish a decentralized trusted communications network independent of any authorization by the host computing device between the host computing device, the first, the second computing device and the third computing device through which digital signals are shared securely between the host computing device, the first user computing device, the second user computing device and the third computing device; **[[and]]**

sending digital signals directly from the host computing device securely to the first, second and third user computing devices since the host computing device and the first, second and third user computing devices have the public key, the host computing device identifiable to the n user computing devices, the n computing devices and the host computing device forming a trusted member list that each computing device has and each computing device knows the other computing devices on the trusted peer-to-peer network[[.]];

sending a search request for a desired computer file from the first user computing device to the other computing devices of the trusted member list via the communication means;

receiving the search request by the second user computing device having the desired file; and

sending the desired computer file to the first user computing device from the second user computing device via the communication means.

Claim 14 (currently amended): A system to establish a trusted and decentralized peer-to peer network comprising:

communication means;

n user computing devices connected to the communication means, where n is greater than or equal to 3 and is an integer; and

a host computing device connected to the communication means having a mechanism to establish a decentralized trusted communications network with at least 3 of the n user computing devices through which digital signals are shared securely between the host computing device and the 3 user computing devices of the trusted communications network, the host computer sending a public key to a first of the 3 user computing devices and the first user computing device sending the public key to a second of the 3 user computer devices and a third of the 3 user devices through the communication means to establish the decentralized trusted network independent of any authorization by the host computing device, the host computing device identifiable to the n user computing devices, the n computing devices and the host computing device forming a trusted member list that each computing device has and each computing device knows and can communicate directly with the other computing devices and the host computing device on the trusted peer-to-peer network since the host computing device and all the other user computing devices have the public key, the first computing device sends a search request to the other computing devices of the trusted member list for a desired computer file via the communication means, the second user computing device having the

desired computer file responds to the search request and sends the desired computer file to the first user computing device.

Claim 15 (previously presented): A method for establishing a trusted and decentralized peer-to-peer network comprising the steps of:

sending a public key from a host computing device to communication means connected to the host computing device;

receiving the public key at a first user computing device of n computing devices, where n is an integer greater than or equal to 3, connected to the communication means;

sending the public key from the first user computing device to a second user computing device connected to the communication means;

sending the public key from the first user computing device to a third user computing device connected to the communication means;

receiving the public key at the third user computing device;

receiving the public key at the second user computing device to establish a decentralized trusted communications network independent of any authorization by the host computing device between the host computing device, the first and the second and the third computing device through which digital signals are shared securely between the host computing device, the first user computing device, the second user computing device and the third computing device;

sending digital signals directly from the host computing device securely to the first, second and third user computing devices since the host computing device and the first, second and third user computing devices have the public key, the host computing device identifiable to the n user computing devices, the n computing devices and the host computing device forming a trusted member list that each computing device has and each computing device knows the other computing devices on the trusted peer-to-peer network; and

establishing entrusted secure chat sessions between the members through the trusted peer-to-peer network.

Claim 16 (previously presented): A method for establishing a trusted and decentralized peer-to-peer network comprising the steps of:

sending a public key from a host computing device to communication means connected to the host computing device;

receiving the public key at a first user computing device of n computing devices, where n is an integer greater than or equal to 3, connected to the communication means;

sending the public key from the first user computing device to a second user computing device connected to the communication means;

sending the public key from the first user computing device to a third user computing device connected to the communication means;

receiving the public key at the third user computing device;

receiving the public key at the second user computing device to establish a decentralized trusted communications network independent of any authorization by the host computing device between the host computing device, the first and the second and the third computing device through which digital signals are shared securely between the host

computing device, the first user computing device, the second user computing device and the third computing device;

sending digital signals directly from the host computing device securely to the first, second and third user computing devices since the host computing device and the first, second and third user computing devices have the public key, the host computing device identifiable to the n user computing devices, the n computing devices and the host computing device forming a trusted member list that each computing device has and each computing device knows the other computing devices on the trusted peer-to-peer network; and

searching for a file by the second user computing device in the first and the third computing devices through the trusted peer-to-peer network.

Claim 17 (previously presented): A method for establishing a trusted and decentralized peer-to-peer network comprising the steps of:

creating encryption and decryption keys;

creating a searchable ciphertext file containing identifiable network information on each computing device which is shared with every other computing device;

sending a public key from a host computing device to communication means connected to the host computing device;

receiving the public key at a first user computing device connected to the communication means;

sending the public key from the first user computing device to a second user computing device connected to the communication means;

receiving the public key at the second user computing device;

either denying or accepting the public key by the second user to establish a decentralized trusted communications network between the host computing device, the first and the second computing device through which digital signals are shared securely between the host computing device, the first user computing device and the second user computing device; and

sending digital signals directly from the first user computing device securely to the second user computing device when the second user computing device has accepted the public key, the host computing device identifiable to the n user computing devices, the n

computing devices and the host computing device forming a trusted member list that each computing device has and each computing device knows the other computing devices on the trusted peer-to-peer network.

Claim 18 (new): A user computing device comprising:

a processor;

storage having a trusted member list of computing devices;

a transceiver that communicates with the computing devices via communication means;

a peer-to-peer network program; and

a crypto API that encrypts and decrypts files, the processor sending a search request for a desired computer file from the transceiver to the other computing devices of the trusted member list via the communication means, and the transceiver receiving the desired computer file from the second user computing device via the communication means.